UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,637	10/12/2001	Verna E. Knapp	10018637 -1	3098

7590 05/31/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
OYEBISI, OJO O	
ART UNIT	**PAPER NUMBER**
3628	

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/976,637	KNAPP ET AL.	
	Examiner	Art Unit	
	OJO O. OYEBISI	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/12/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 3-7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 3 recites the phrase "For a commerce system comprising" in the preamble. The language of this phrase is indefinite in that it fails to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Appropriate correction is required. Claims 4-7 are rejected because of their dependency from the rejected claim 3.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claim 1-11 are rejected under 35 U.S.C. 102(b) as being anticipated by Krsul et al (Krsul hereinafter, US PAT: 5,839,119).

Re claims 1. Krsul discloses a computer-readable medium having stored thereon a data structure comprising: information identifying a secret share of a finite set of secret shares (i.e., Bank 18 makes an entry in this database for every buyer-seller pair with outstanding, valid electronic tokens. Bank 18 assigns a unique identifier, which we shall call a purse identifier, to the group of electronic tokens just generated. Banks 18 then notes the purse identifier in its database entry for this buyer-seller pair, as well as all of the session serial numbers of those electronic tokens. Bank 18 also stores the address of seller 17 in the database entry in case buyer 16 should wish to redeem unspent electronic token halves. That done, bank 18 advances to step 1026 from step 1025, see col.8 lines 17-45, specifically see col.8 lines 35-45, also see col.2 lines 19-48); and a secret share profile associated with the secret share and comprising a set of activities associated with the secret share, the set of activities corresponding to at least one activity conducted within a commerce system by at least a portion of a plurality of entities within the commerce system (i.e., the present invention result from splitting the electronic tokens in half using secret splitting. Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces. None of the parties to the secret can learn the secret without all cooperating with one another to combine their secret pieces. Each secret piece is valueless on its own, as well as meaningless to anyone without all the other secret pieces. Because each electronic token half is valueless by itself, buyer 16 is protected from unauthorized redemptions of electronic tokens by seller 17. When session serial numbers are added to the electronic token halves, both bank 18 and buyer 17 are protected from double spending. Referring

again to FIGS. 4A and 4B, for simplicity steps 1018-1024 show only one electronic token being split in half at a time; however, the present invention is consistent with many electronic tokens being split at once. First, during step 1020, bank 18 selects one of the signed electronic tokens to be split using secret splitting, see col.7 lines 45-65, also see col.2 lines 19-48) (see the summary of the invention and the abstract)

Re claims 2. Claim 2 recites similar limitations to claim 1 and thus rejected using the same art and rationale in the rejection of claim 1.

Re claims 3-5. Krsul further discloses For a commerce system comprising a plurality of entities each having an associated entity identity that is stored as a plurality of secret shares amongst at least a portion of a plurality of shareholders (buyers and sellers) (i.e., Bank 18 makes an entry in this database for every buyer-seller pair with outstanding, valid electronic tokens. Bank 18 assigns a unique identifier, which we shall call a purse identifier, to the group of electronic tokens just generated. Banks 18 then notes the purse identifier in its database entry for this buyer-seller pair, as well as all of the session serial numbers of those electronic tokens. Bank 18 also stores the address of seller 17 in the database entry in case buyer 16 should wish to redeem unspent electronic token halves. That done, bank 18 advances to step 1026 from step 1025, see col.8 lines 17-45, specifically see col.8 lines 35-45, also see col.2 lines 19-48), wherein each plurality of secret shares comprises a subset of a finite set of secret share values (i.e. Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces, see col.7 lines 45-55, also see col.2 lines 18-48), a method for estimating activities of a first entity of the plurality of entities, the method

comprising: associating, for each entity of the plurality of entities, at least one activity conducted by the entity within the commerce system with each of the plurality of secret shares used to store the entity identity corresponding to the entity such that each secret share of the finite set of secret share values has associated therewith a set of activities from at least a portion of the plurality of entities; and generating, for the first entity, an estimated activities list comprising an intersection of sets of activities associated with each secret share of a first plurality of secret shares used to store a first entity identity corresponding to the first entity (i.e., Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces. None of the parties to the secret can learn the secret without all cooperating with one another to combine their secret pieces. Each secret piece is valueless on its own, as well as meaningless to anyone without all the other secret pieces. Because each electronic token half is valueless by itself, buyer 16 is protected from unauthorized redemptions of electronic tokens by seller 17. When session serial numbers are added to the electronic token halves, both bank 18 and buyer 17 are protected from double spending. Referring again to FIGS. 4A and 4B, for simplicity steps 1018-1024 show only one electronic token being split in half at a time; however, the present invention is consistent with many electronic tokens being split at once. First, during step 1020, bank 18 selects one of the signed electronic tokens to be split using secret splitting, see col.7 lines 45-65, also see col.2 lines 18-48) (see the abstract and the summary of the invention).

Re claim 6. Krsul further discloses the method wherein generating the estimated activities list further comprises: retrieving, by an anonymity service provider in

communication with the first entity and each of the first portion of the plurality of shareholders (i.e., providing anonymity to buyer, and preventing sellers from building a dossier about the buyer, see col.6 lines 40-48), the plurality of profiles from the first portion of the plurality of shareholders; and calculating, by the anonymity service provider, the intersection by determining common activities that are found within each of the plurality of profiles (i.e., using its computer network bank 18 generates a first token half for the buyer. This is done by generating a random electronic string P whose bit length is equal to that of the selected signed token. The random string P is then used to create the second token half for the signed electronic token. Using its computer network, bank 18 generates the second electronic token half, Q, by performing a bitwise XOR of S.sub.BP (T) and P, resulting in Q. Neither the first electronic token half, P, nor the second electronic token half, Q, have any value of themselves; however, they can be combined together by a bitwise XOR to obtain S.sub.BP (T). This prevents seller 17 from redeeming tokens without the consent of buyer 16, as well as protecting seller 17 from double-spending by buyer 16. Note also, that buyer 16 can use her electronic tokens only for purchases with the selected seller. If she wishes to do business with another seller, she must obtain another, different set of token halves, col.8 lines 1-15).

Re claim 7. Krsul further discloses the method of claim 3, wherein the at least one activity includes purchase of at least one digital product (i.e., Note also, that buyer 16 can use her electronic tokens only for purchases with the selected seller. If she wishes

to do business with another seller, she must obtain another, different set of token halves, col.8 lines 5-15).

Re claims 8-10. Krsul further discloses an apparatus for use in a commerce system comprising a plurality of entities each having an associated entity identity that is stored as a plurality of secret shares amongst at least a portion of a plurality of shareholders (i.e., the present invention result from splitting the electronic tokens in half using secret splitting. Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces. None of the parties to the secret can learn the secret without all cooperating with one another to combine their secret pieces. Each secret piece is valueless on its own, as well as meaningless to anyone without all the other secret pieces. Because each electronic token half is valueless by itself, buyer 16 is protected from unauthorized redemptions of electronic tokens by seller 17. When session serial numbers are added to the electronic token halves, both bank 18 and buyer 17 are protected from double spending, see col.7 lines 45-65, see col.2 lines 18-48, also see **the abstract** for secret splitting of electronic token between buyers and sellers), wherein each plurality of secret shares comprises a subset of a finite set of secret share values (i.e. Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces, see col.7 lines 45-55, also see col.2 lines 18-48), the apparatus comprising: means for associating, for each entity of the plurality of entities, at least one activity conducted by the entity within the commerce system with each of the plurality of secret shares used to store the entity identity corresponding to the entity such that each secret share of the finite set of secret share values has associated

therewith a set of activities from at least a portion of the plurality of entities; means for receiving sets of activities associated with each secret share of a first plurality of secret shares used to store a first entity identity corresponding to a first entity; and means, coupled to the means for receiving, for generating an estimated activities list, for the first entity, comprising an intersection of the sets of activities (i.e., Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces. None of the parties to the secret can learn the secret without all cooperating with one another to combine their secret pieces. Each secret piece is valueless on its own, as well as meaningless to anyone without all the other secret pieces. Because each electronic token half is valueless by itself, buyer 16 is protected from unauthorized redemptions of electronic tokens by seller 17. When session serial numbers are added to the electronic token halves, both bank 18 and buyer 17 are protected from double spending. Referring again to FIGS. 4A and 4B, for simplicity steps 1018-1024 show only one electronic token being split in half at a time; however, the present invention is consistent with many electronic tokens being split at once. First, during step 1020, bank 18 selects one of the signed electronic tokens to be split using secret splitting, see col.7 lines 45-65, also see col.2 lines 18-48) (see the abstract and the summary of the invention).

Re claim 11. Claim 11 recites similar limitations to claim 6 and thus rejected using the same art and rationale in the rejection of claim 6.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OJO O. OYEBISI whose telephone number is (571) 272-8298. The examiner can normally be reached on 8:30A.M-5:30P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, HYUNG S. SOUGH can be reached on (571)272-6799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

***

HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600